



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/741,406	12/19/2000	James W. Edwards	10559/295001/P9306	6308
20985	7590	01/27/2005	EXAMINER	
FISH & RICHARDSON, PC 12390 EL CAMINO REAL SAN DIEGO, CA 92130-2081			REVAK, CHRISTOPHER A	
			ART UNIT	PAPER NUMBER

2131

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/741,406	<b>Applicant(s)</b> EDWARDS ET AL.	
	<b>Examiner</b> Christopher A. Revak	<b>Art Unit</b> 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 02 October 2004.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-3,5-12,14-26 and 28 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-3,5-12,14-26 and 28 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION*****Response to Arguments***

1. Applicant's arguments filed October 4, 2004 have been fully considered but they are not persuasive.

It is argued by the applicant that Gilbrech does not teach a server as being a second component, but instead the second component is a router as per the teachings of Gilbrech. The examiner respectfully disagrees. Based upon the applicant's disclosure, the server component allows the client to connect over two or more networks, provides for temporary connections such as a virtual connection path, and additionally, the server component supports use of user accounts and passwords and is responsible for authentication for access to the private network as is recited on page 5, lines 5-7, 9-11, and lines 17-20. As per the teachings of Gilbrech, the term "server" is not disclosed, however the functionality of the virtual private network unit, or VPN Units, performs the same functions of a "server component" as indicated in the applicant's specification as recited above. Figure 2 demonstrates a client the ability to connect over two or more LANS (private networks) across the public network. Gilbrech discloses that a virtual private network is used, and VPNs are known to exist as temporary connections, see column 2, lines 45-50. Gilbrech additionally discloses that the VPN Units are responsible for the enforcement of rules and authentication practices as are applied to the group members, see column 2, lines 58-64.

The applicant has argued that "a connection lasting as long as a mechanism at each of the components supporting a connection remains active" is not taught by

Art Unit: 2131

Gilbrech. The examiner respectfully disagrees. The applicant has recited in the specification virtual path connections are temporary connections as is recited on page 5, lines 9-11 which is consistent with virtual private networks only maintaining the connection as long as the tunnel is established between two endpoints. Termination can occur when the devices terminate the connection or keys can expire causing the connection to terminate.

The applicant has indicated that the examiner's interpretation is inconsistent for independent claims 1 and 10 versus independent claim 19. The examiner has reconstructed the rejection so that they are now similarly applied.

2. The applicant has complied with overcoming the examiner's objection to the specification and the objection is hereby withdrawn.

***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-3,5-12,14-26, and 28 are rejected under 35 U.S.C. 102(e) as being anticipated by Gilbrech et al.

As per claim 1, it is disclosed by Gilbrech et al of a method comprising sending a packet originating from a source (device) across the Internet (public network) to a

Art Unit: 2131

receiving VPN Unit (second/server component) to establish a connection between the source (device) and a LAN (private network)(col. 6, lines 38-41; col. 8, lines 29-55; and as shown in Figures 2 & 5). The router (first component) is configured to connect to the VPN Unit (second/server component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2). It is determined if the communications from the device conform to authentication (authorization) rules to connect with the LAN (private network)(col. 2, lines 57-67). The request initiates from a router (first component) and is forwarded to a VPN Unit (second/server component) to establish the connection with the destination (col. 2, lines 43-53, 57-67 & col. 8, lines 17-26). The router (first component) creates and establishes the connection between the LAN (private network) and source (device) via the VPN Unit (second/server component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5). The examiner notes that routers are known as devices that receive transmitted messages and forward them to their correct destination, namely the LAN (private network) in light of the teachings of Gilbrech et al (as shown in Figures 2 & 5). The router (first component) is configured to connect to the VPN Unit (second/server component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2).

As per claims 2 and 11, Gilbrech et al discloses of forwarding a request initiated by a router (first component) and is forwarded to a VPN Unit (second/server component) to establish the connection with the destination (col. 2, lines 43-53, 57-67 & col. 8, lines 17-26). The examiner is interpreting the connection between the source (device), VPN Unit (second device), router (first network component), and device(s) on the LAN

Art Unit: 2131

(private network) to remain active as long as the devices maintain communications with one another and that the connection is temporary until terminated.

As per claims 3 and 12, Gilbrech et al discloses of determining if the communications from the device conform with authentication rules to connect with the LAN and if so forwarding a request initiated by a router (first component) and is forwarded to a VPN Unit (second/server component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). If the request is not from a recognized member of the VPN group, the packets are discarded (denying the device access)(col. 2, lines 57-67 & col. 8, lines 12-27).

As per claims 5,6,14,15,25, and 26, it is disclosed by Gilbrech et al of a method comprising sending a packet originating from a source (device) across the Internet (public network) to a receiving VPN Unit (second/server component) to establish a connection between the source (device) and a LAN (private network)(col. 6, lines 38-41; col. 8, lines 29-55; and as shown in Figures 2 & 5). The router (first component) is configured to connect to the VPN Unit (second/server component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2). It is determined if the communications from the device conform to authentication (authorization) rules to connect with the LAN (private network)(col. 2, lines 57-67). The request initiates from a router (first component) and is forwarded to a VPN Unit (second/server component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). The router (first component) creates and establishes the connection between the LAN (private network) and source (device) via the VPN Unit (second/server component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures

Art Unit: 2131

2 & 5). The examiner is interpreting the connection between the source (device), VPN Unit (first network component), and router (second network component) to remain active as long as the devices maintain communications with one another unless if that connection is terminated by any or all of the devices.

As per claims 7 and 16, Gilbrech et al discloses of determining if the communications from the device conform to authentication (authorization) rules to connect with the LAN (private network)(col. 2, lines 57-67). The request initiates from a router (first component) and is forwarded to a VPN Unit (second/server component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). The examiner is interpreting the authentication rules to include a password since passwords are generally used for authentication.

As per claims 8, 17, and 23, it is recited by the teachings of Gilbrech et al that the public network includes the Internet (col. 2, lines 43-46).

As per claims 9 and 18, Gilbrech et al teaches of determining if the communications from the device conform to authentication (authorization) rules to connect with the LAN (private network)(col. 2, lines 57-67). The request initiates from a router (first component) and is forwarded to a VPN Unit (second/server component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). It is interpreted by the examiner that the VPN Unit (second/server component) and router (first network component) are proxy servers since it is disclosed in the applicant's specification "Proxy servers can monitor and intercept any and all requests being sent to and/or received from the private network and/or the Internet. The proxying components can also provide client-to-private-network encryption" as is recited on page 7, lines 13-

Art Unit: 2131

17. Gilbrech discloses of performing encryption services on the packets and shows how both the VPN Unit (second/server network component) and router (first network component) intercept communications since that is the only path into the LAN (private network)(col. 8, lines 19-26 & as shown in Figure 2).

As per claim 10, it is disclosed by Gilbrech et al of a techniques (machine readable instructions stored on an article) for sending a packet originating from a source (device) across the Internet (public network) to a receiving VPN Unit (second/server component) to establish a connection between the source (device) and a LAN (private network)(col. 6, lines 38-41; col. 8, lines 29-55; and as shown in Figures 2 & 5). The router (first component) is configured to connect to the VPN Unit (second/server component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2). It is determined if the communications from the device conform to authentication (authorization) rules to connect with the LAN (private network)(col. 2, lines 57-67). The request initiates from a router (first component) and is forwarded to a VPN Unit (second/server component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). The router (first component) creates and establishes the connection between the LAN (private network) and source (device) via the VPN Unit (second/server component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5). The examiner notes that routers are known as devices that receive transmitted messages and forward them to their correct destination, namely the LAN (private network) in light of the teachings of Gilbrech et al (as shown in Figures 2 & 5). The router (first component) is configured to connect to the



Art Unit: 2131

VPN Unit (second/server component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2).

As per claim 19, it is disclosed by Gilbrech et al of a system for sending a packet originating from a source (device) across the Internet (public network) to a receiving VPN Unit (server component) to establish a connection between the source (device) and a LAN (private network)(col. 6, lines 38-41; col. 8, lines 29-55; and as shown in Figures 2 & 5). The VPN Unit (server component) establishes the connection with the destination (col. 2, lines 57-67 & col. 8, lines 17-26). The request is then forwarded from the VPN Unit (server component) to the router (agent)(col. 8, lines 52-55 & as shown in Figures 2 & 5). The router (agent) creates and establishes the connection between the LAN (private network) and source (device) via the VPN Unit (server component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5). The examiner notes that routers are known as devices that receive transmitted messages and forward them to their correct destination, namely the LAN (private network) in light of the teachings of Gilbrech et al (as shown in Figures 2 & 5). The router (agent component) is configured to connect to the VPN Unit (server component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2).

As per claim 20, Gilbrech et al discloses of a router (agent) that creates and establishes the connection between the LAN (private network) and source (device) via the VPN Unit (server component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5). The examiner notes that routers are known as devices that receive transmitted messages and forward them to their correct destination, namely the any

Art Unit: 2131

devices within the LAN (private network) as is taught by Gilbrech et al (as shown in Figures 2 & 5).

As per claims 20 and 21, Gilbrech et al teaches of forwarding a request from the VPN Unit (server component) to the router (agent)(col. 8, lines 52-55 & as shown in Figures 2 & 5). The router (agent) creates and establishes the connection (by providing access) between the LAN (private network) and source (device) via the VPN Unit (server component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5). Figure 2 shows multiple devices connected to the LAN (private network).

As per claim 22, it is disclosed by Gilbrech et al that communications are extensible to support any protocol used by the Internet (public network) and the LAN (private network)(col. 5, lines 57-61 & col. 6, lines 5-22). It is interpreted by the examiner that the VPN Unit (server component) and router (agent) handle the different protocols since they are connected across the Internet (public network) and LAN (private network)(as shown in Figures 2 & 5).

As per claim 24, Gilbrech et al teaches of determining if the communications from the device conform to authentication rules to connect with the LAN and if so, the VPN Unit (server component) establishes the connection with the destination (col. 2, lines 57-67 & col. 8, lines 17-26).

As per claims 27 and 29, Gilbrech et al teaches of determining if the communications from the device conform to authentication (authorization) rules to connect with the LAN and if so, the VPN Unit (server component) establishes the connection with the destination (col. 2, lines 57-67 & col. 8, lines 17-26). The request is then forwarded from the VPN Unit (server component) to the router (agent)(col. 8, lines

Art Unit: 2131

52-55 & as shown in Figures 2 & 5). It is interpreted by the examiner that the VPN Unit (server component) and router (agent) are proxy servers since it is disclosed in the applicant's specification "Proxy servers can monitor and intercept any and all requests being sent to and/or received from the private network and/or the Internet. The proxying components can also provide client-to-private-network encryption" as is recited on page 7, lines 13-17. Gilbrech discloses of performing encryption services and authentication rules (security mechanisms) on the packets and shows how both the VPN Unit (server component) and router (agent) intercept communications since that is the only path into the LAN (private network)(col. 8, lines 19-26 & as shown in Figure 2).

As per claim 28, it is shown in Figure 2 of Gilbrech et al the routers (agents) are implemented inside the LANs (private networks).

### ***Conclusion***

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

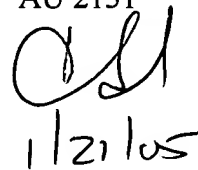
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak

AU 2131

  
1/21/05CR 

January 21, 2005